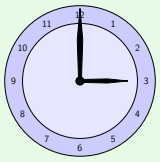
Modulo-Rechnung

Schlüsselaustausch

Um einen Klartext zu verschlüsseln und auch anschließend zu entschlüsseln, brauchen Sender und Empfänger denselben Schlüssel. Dieser ist meist eine Zahl. Sender und Empfänger müssen den Schlüssel **geheim** austauschen können, das heißt, ohne dass ein Dritter ihn erfährt.

Der geheime Schlüsselaustausch erfordert oft einige Rechenoperationen beim Sender wie auch beim Empfänger. Modulo ist eine Rechenoperation (wie z. B. Addition oder Multiplikation). Sie wird für zahlreiche Verschlüsselungsverfahren und Schlüsselaustausch-Verfahren benötigt. Auch der Diffie-Hellman-Algorithmus arbeitet mit der Modulo-Operation.
Die Modulo-Operation ist aber leicht zu verstehen.
Mit Modulo, **mod**, wird einfach der Rest der ganzzahligen Division bezeichnet.

Beispiel



Jeder von uns benutzt fast täglich die Modulo-Rechnung. Die kommt nämlich bei der Berechnung der Uhrzeit vor. Wir sagen zu der Uhrzeit 15:00 Uhr meist 3 Uhr (nachmittags). Das ist die Modulo-Rechnung mit der Zahl 12: $15 \; mod \; 12 \; = \; 3$, da $15 \; : \; 12 \; = \; 1, \quad \mathbf{3}$ bleibt übrig.

Natürlich rechnet man nicht immer $mod \; 12$. 12 kann durch jede ganze Zahl ersetzt werden. Bei den meisten Verschlüsselungsverfahren kommen keine negativen Zahlen vor, das macht es etwas einfacher.

Beispiel

Rechnungen

$18 \; mod \; 5 \; = \; 3$, da $18 \; : \; 5 \; = \; 3$ **(Rest 3)**

$10 \; mod \; 4 \; = \; 2$, da $10 \; : \; 4 \; = \; 2$ **(Rest 2)**

$14 \; mod \; 7 \; = \; 0$, da $14 \; : \; 7 \; = \; 2$ **(Rest 0)**